

On the Communication Cost of Determining an Approximate Nearest Lattice Point

Maiara F. Bollauf^{*}, Vinay A. Vaishampayan[†] and Sueli I. R. Costa[‡]

^{*} [‡] Institute of Mathematics, Statistic and Computer Science
University of Campinas, Sao Paulo, Brazil
Email: maiarabollauf@ime.unicamp.br, sueli@ime.unicamp.br

[†] Department of Engineering Science and Physics
College of Staten Island, City University of New York, Staten Island - NY, United States
Email: Vinay.Vaishampayan@csi.cuny.edu

Abstract—We consider the closest lattice point problem in a distributed network setting and study the communication cost and the error probability for computing an approximate nearest lattice point, using the nearest-plane algorithm, due to Babai. Two distinct communication models, centralized and interactive, are considered. The importance of proper basis selection is addressed. Assuming a reduced basis for a two-dimensional lattice, we determine the approximation error of the nearest plane algorithm. The communication cost for determining the Babai point, or equivalently, for constructing the rectangular nearest-plane partition, is calculated in the interactive setting. For the centralized model, an algorithm is presented for reducing the communication cost of the nearest plane algorithm in an arbitrary number of dimensions.

Index terms—Lattices, lattice quantization, distributed function computation, communication complexity.

I. INTRODUCTION

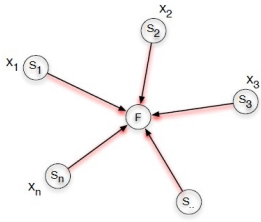


Fig. 1. Centralized model

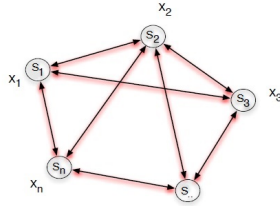


Fig. 2. Interactive model

Consider a generic distributed function computation problem in a network of N interconnected sensor/computers and possibly a central computing node, called a fusion center F . Communication links with limited bandwidth interconnect the nodes, which are assumed to have limited processing power. Node i observes real valued random variable X_i . In the *centralized model* (Fig. 1), the objective is to compute a function $f(x_1, x_2, \dots, x_n)$ at the fusion center by communicating information from the nodes. We also consider the *interactive model* (Fig. 2), where the purpose is to compute a function $f(x_1, x_2, \dots, x_n)$ at each node, and the fusion center is absent. In general, since random variables are real valued, these calculations would require that the system communicate

an infinite number of bits. Since the network has finite bandwidth links, the information must be quantized in a suitable manner, but quantization affects the accuracy of the function that we are trying to compute. Thus, the main goal is to manage the tradeoff between communication cost and function computation accuracy.

Here, f computes the closest lattice point in a given lattice Λ to a real vector $x = (x_1, x_2, \dots, x_n)$. This process is widely used for decoding lattice codes, and for quantization. Lattice coding offers significant coding gains [5] for noisy channel communication and for quantization, leads to performance approaching the rate distortion bound [4] for some sources and distortion measures.

In both models, n sensor-processor nodes, S_1, S_2, \dots, S_n are available and node S_i observes a real-valued, discrete-time random signal represented by the iid random process $\{X_i(t), t \in \mathbb{Z}\}$, where t denotes the time index. The probability density function of X_i is denoted p_i . It is also assumed that $X_i(t)$ is independent of $X_j(t')$, $(i, t) \neq (j, t')$. The objective is to compute the function $f : \mathbb{R}^n \rightarrow \Lambda$, which maps a realization at time t , $x(t) = (x_1(t), x_2(t), \dots, x_n(t))$ to the nearest vector in a lattice $\Lambda \subset \mathbb{R}^n$ with basis $\{v_1, v_2, \dots, v_n\}$. For most of this paper, we will drop the time index t and write x instead of $x(t)$.

Problems in distributed function computation [2] arise in a broad range of modern settings, e.g. network MIMO systems for next generation wireless networks [15] and network management in wide area networks [8]. For prior work in the computer science community, see [18], [9]. Information theory [16] has resulted in tight bounds, [13], [11]. A comprehensive survey and novel algorithms for the closest lattice point problem are in [1]. The communication cost/error tradeoff of refining the nearest-plane estimate is addressed in a companion paper [17].

The remainder of our paper is organized into three sections: Sec. II presents some basic definitions, previous work related to communication complexity and establishes a framework for measuring the cost and error rate. Sec. III is where we exhibit our contributions, i.e., an expression for probability of error of the distributed closest lattice point problem in an arbitrary

two-dimensional case and estimations of the rate calculation in both models. Sec. IV presents conclusions and directions for future work.

II. LATTICE BASICS, PARTITIONS, RATES AND DISTORTIONS

Notation and essential aspects of lattice coding are described in this section.

Definition 1. (Lattice) A lattice $\Lambda \subset \mathbb{R}^M$ is the set of integer linear combinations of independent vectors $v_1, v_2, \dots, v_n \in \mathbb{R}^M$, with $n \leq M$,

Definition 2. (Generator matrix) The generator matrix of the lattice is represented by matrix V with i th column v_i , $i = 1, 2, \dots, n$. Thus $\Lambda = \{Vu, u \in \mathbb{Z}^n\}$, where u is considered here as a column vector.

We will assume in the sequence of our work that Λ has full rank ($n = M$).

Definition 3. (Voronoi cell and relevant vectors) The Voronoi cell $\mathcal{V}(\lambda)$ of a lattice $\Lambda \subset \mathbb{R}^n$ is the subset of \mathbb{R}^n containing all points nearer to lattice point λ than to any other lattice point. The relevant vectors of a lattice Λ are those which contribute to determine a face of the Voronoi cell.

The closest vector problem (CVP) in a lattice can be described as an integer least squares problem with the objective of determining u^* , such that

$$u^* = \arg \min_{u \in \mathbb{Z}^n} \|x - Vu\|^2, \quad (1)$$

where the norm considered is the standard Euclidean norm. The closest lattice point to x is then given by $x_{nl} = Vu^*$. The mapping $g_{nl} : \mathbb{R}^n \rightarrow \Lambda$, $x \mapsto x_{nl}$ partitions \mathbb{R}^n into Voronoi cells, each of volume $|\det V|$.

The nearest plane (np) algorithm computes x_{np} , an approximation to x_{nl} , given by $x_{np} = b_1v_1 + b_2v_2 + \dots + b_nv_n$, where $b_i \in \mathbb{Z}$ is obtained as follows, derived from [3].

Let \mathcal{S}_i denote the subspace spanned by the vectors $\{v_1, v_2, \dots, v_i\}$, $i = 1, 2, \dots, n$. Let $\mathcal{P}_i(z)$ be the orthogonal projection of z onto \mathcal{S}_i and let $v_{i,i-1} = \mathcal{P}_{i-1}(v_i)$ be the nearest vector to v_i in \mathcal{S}_{i-1} . We have the following unique decomposition: $v_i = v_{i,i-1} + v_{i,i-1}^\perp$. Also, let $z_i^\perp = z_i - \mathcal{P}_i(z_i)$. Start with $z_n = x$ and $i = n$ and compute $b_i = \lceil \langle z_i, v_{i,i-1}^\perp \rangle / \|v_{i,i-1}^\perp\|^2 \rceil$, $z_{i-1} = \mathcal{P}_{i-1}(z_i) - b_iv_{i,i-1}$, for $i = n, n-1, \dots, 1$. Here $\lceil x \rceil$ denotes the nearest integer to x .

The mapping $g_{np} : \mathbb{R}^n \rightarrow \Lambda$, $x \mapsto x_{np}$, partitions \mathbb{R}^n into hyper-rectangular cells with volume $|\det V|$, as illustrated in Fig. 3 for the hexagonal lattice A_2 . We refer to this partition as a *Babai* partition. Note that this partition is basis dependent. In case V is upper triangular with (i, j) entry v_{ij} , each rectangular cell is axis-aligned and has sides of length $|v_{11}|, |v_{22}|, \dots, |v_{nn}|$.

In this work, we will assume that the underlying basis for \mathbb{R}^n is chosen in such a way that V is a upper triangular matrix. This can be accomplished by applying the QR decomposition to any given generator matrix. Note that since Q is an

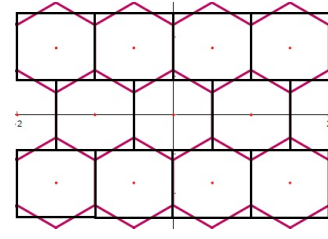


Fig. 3. Cells of the *np* or *Babai* partition (black boundaries) and the Voronoi partition (pink solid lines) of \mathbb{R}^2 for hexagonal lattice A_2 with basis $\{(1, 0), (1/2, \sqrt{3}/2)\}$

orthogonal matrix, the matrix R can be viewed either as having for its columns the basis vectors of the original lattice written in this new coordinate frame or as the basis vectors of a lattice congruent to the original one.

As will be discussed in Sec. III the efficiency of the *np*-algorithm is strongly related to the choice of a starting good basis.

Definition 4. (Minkowski-reduced basis [12]) A basis $\{v_1, v_2, \dots, v_n\}$ of a lattice Λ in \mathbb{R}^n is said to be Minkowski-reduced if v_j , with $j = 1, \dots, n$, is such that $\|v_j\| \leq \|v\|$, for any v for which $\{v_1, \dots, v_j, v\}$ can be extended to a basis of Λ .

In particular, for lattices of dimension $n \leq 4$, the norm of the Minkowski-reduced basis vectors achieve the successive minima [14]. For two dimensional lattices, a Minkowski-reduced basis is also called Lagrange-Gauss reduced basis and there is a simple characterization [5], which states that: a lattice basis $\{v_1, v_2\}$ is a Minkowski-reduced basis if only if $\|v_1\| \leq \|v_2\|$ and $2 < v_1, v_2 \leq \|v_1\|^2$.

From this result we can deduce that the angle θ between the minimum norm vector v_1 and v_2 must satisfy $\frac{\pi}{3} \leq \theta \leq \frac{2\pi}{3}$.

The partition constructed by the *np*-algorithm is basis dependent. Since a Minkowski-reduced basis consists of short vectors that are “as perpendicular as possible”, it is a good choice for starting the *np*-algorithm. But it is computationally hard to get such basis from arbitrary ones. One alternative is to use the basis obtained with the LLL algorithm [10], which approximates the Minkowski bases and can be achieved in polynomial time. For a basis that is LLL reduced, the ratio of the distances $\|x - x_{np}\| / \|x - x_{nl}\|$ can be bounded above by a constant that depends on the dimension alone [3].

III. EXPLORING THE DISTRIBUTED PROBLEM IN AN ARBITRARY TWO-DIMENSIONAL LATTICE

We will assume that the lattice Λ is generated by the scaled generator matrix αV , where V is the generator matrix of the unscaled lattice. Our analysis will proceed under the assumption that α is sufficiently small. Let $\mathcal{V}(\lambda)$ and $\mathcal{B}(\lambda)$ denote the Voronoi and Babai cells, respectively, associated with lattice vector $\lambda \in \Lambda$. The error probability P_e , is the probability of the event $\{\lambda_{nl}(X) \neq \lambda_{np}(X)\}$ and is given by $P_e \approx \text{area}(\mathcal{B}(0) \cap \mathcal{V}(0)^c) / \text{area}(\mathcal{B}(0))$ for α sufficiently

small. We provide an error analysis in Sec. III-A and a rate analysis in Sec. III-B

A. Error Analysis: (Babai \times Voronoi)

A Babai partition is basis dependent whereas the Voronoi partition is independent of the basis used to represent the lattice. This has an impact on the error probability. To better illustrate this, consider the following example.

Example 1. Consider a lattice $\Lambda \subset \mathbb{R}^2$ with basis $\{(5,0), (3,1)\}$. The probability of error in this case is $P_e = 0.6$ (Fig. 4), whereas if we start from the basis $\{(1,2), (-2,1)\}$, we achieve after the QR decomposition $\{(\sqrt{5},0), (0,\sqrt{5})\}$ and $P_e = 0$, since the Babai region associated with an orthogonal basis and the Voronoi region for rectangular lattices coincides.

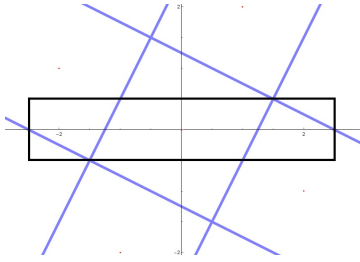


Fig. 4. Voronoi region and Babai partition of the triangular basis $\{(5,0), (3,1)\}$

Example 1 illustrates the necessity of working with a good basis. In our analysis, we will always consider a Minkowski-reduced basis.

An equivalent condition for a Minkowski-reduced basis in dimension two is $\|v_1\| \leq \|v_2\| \leq \|v_1 \pm v_2\|$ from which the following result can be derived [6].

Lemma 1. If a Minkowski-reduced basis is particularly given by $\{(1,0), (a,b)\}$ then, besides the basis vectors, a third relevant vector is

$$\begin{cases} (-1+a, b), & \text{if } \frac{\pi}{3} \leq \theta \leq \frac{\pi}{2} \\ (1+a, b), & \text{if } \frac{\pi}{2} < \theta \leq \frac{2\pi}{3}. \end{cases} \quad (2)$$

Note that, if $\{v_1, v_2\}$ is a Minkowski basis then so is $\{-v_1, v_2\}$ and hence any lattice has a Minkowski basis with $\frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}$. Thus, up to congruence and a scaling factor (which produces equivalent lattices), a Minkowski-reduced basis of a lattice $\Lambda \subseteq \mathbb{R}^2$ can always be considered to be in the form $\{(1,0), (a,b)\}$, with $a^2 + b^2 \geq 1$ and $0 \leq a \leq \frac{1}{2}$. So, we can use Lemma 1 to describe the Voronoi region of Λ and determine its intersection with the associated Babai partition. Note that the area of both regions must be the same and in this specific case, equal to b . This means that the vertices that define the Babai rectangular partition are $(\pm \frac{1}{2}, \pm \frac{b}{2})$.

Theorem 1. Consider an arbitrary lattice $\Lambda \subset \mathbb{R}^2$ with a Minkowski-reduced basis given by $\gamma = \{v_1, v_2\}$ such that the angle θ between v_1 and v_2 satisfies $\frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}$.

By QR decomposition, we can obtain a triangular basis $\beta = \{(1,0), (a,b)\}$ which generates a congruent lattice to the one generated by γ . Then, the probability of error P_e regarding the Babai partition is given by

$$P_e = F(a, b) = \frac{a - a^2}{4b^2}. \quad (3)$$

Proof: Since the lattice generated by β is a scaling factor of γ , we must have the same P_e associated to the correspondent lattices. The two inequalities regarding a and b are derived from the fact that the QR decomposition is done through an orthogonal matrix which preserves the inner product and hence the Minkowski-reduced condition also holds for the bases β and γ .

To calculate P_e for the lattice Λ we consider the three relevant vertices $(1,0)$, (a,b) and $(-1+a, b)$ (according to Lemma 1, Fig. 5) of the Voronoi region, determine for each of these points the equidistant straight line to the origin and obtain from the intersection of these lines the Voronoi polyhedron vertices $\pm(\frac{1}{2}, \frac{a^2+b^2-a}{2b})$, $\pm(-\frac{1}{2}, \frac{a^2+b^2-a}{2b})$ and $\pm(\frac{2a-1}{2}, \frac{-a^2+b^2+a}{2})$.

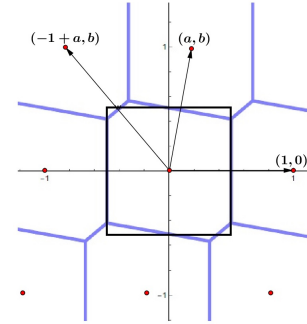


Fig. 5. Voronoi region, Babai partition and three relevant vectors

P_e is then computed as the ratio between the area of the Babai region which is not overlapped by the Voronoi region $\mathcal{V}(0)$ and the area $|b|$ of the Babai region. From Fig. 5, we get the error as the sum the areas of four triangles, where two of them are defined respectively by the points $(\frac{1}{2}, \frac{b}{2})$, $(\frac{1}{2}, \frac{a^2-a+b^2}{2b})$, $(\frac{a}{2}, \frac{b}{2})$ and $(-\frac{1}{2}, \frac{b}{2})$, $(-\frac{1}{2}, \frac{a^2-a+b^2}{2b})$, $(\frac{a-1}{2}, \frac{b}{2})$. The remaining two triangles are symmetric to these two. Therefore, the probability of error is the sum of the four areas, normalized by the area of the Voronoi region $|\det(V)| = |b|$. The explicit formula for it is given by $F(a, b) = \frac{1}{4} \frac{a - a^2}{b^2}$. ■

Remark 1. Note also that starting from any Minkowski-reduced basis of a two dimensional lattice $\gamma = \{v_1, v_2\}$, considering $\rho = \frac{\|v_2\|}{\|v_1\|}$ and the angle θ between the basis vectors, then the result of Theorem 1 can be rewritten as

$$P_e = H(\theta, \rho) = \frac{1}{4\rho} \frac{|\cos \theta|}{\sin^2 \theta} (1 - \rho |\cos \theta|). \quad (4)$$

Since, from Theorem 1 the probability of error $P_e = F(a, b) = \frac{1}{4} \frac{a}{b^2} (1 - a) = \frac{1 - (1 - 2a)^2}{16b^2}$ and taking into account that $b \geq \frac{\sqrt{3}}{2}$ and $0 \leq a \leq \frac{1}{2}$, we obtain the following Corollary, illustrated in Fig. 6.

Corollary 1. *For any two dimensional lattice and a Babai partition constructed from the QR decomposition associated with a Minkowski-reduced basis where $\frac{\pi}{3} \leq \theta \leq \frac{\pi}{2}$, we have*

$$0 \leq P_e \leq \frac{1}{12}, \quad (5)$$

and

- a) $P_e = 0 \iff a = 0$, i.e., the lattice is orthogonal.
- b) $P_e = \frac{1}{12} \iff (a, b) = \left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$, i.e., the lattice equivalent to hexagonal lattice.
- c) the level curves of P_e are described as ellipse arcs in the region $a^2 + b^2 \geq 1$ and $0 \leq a \leq \frac{1}{2}$.

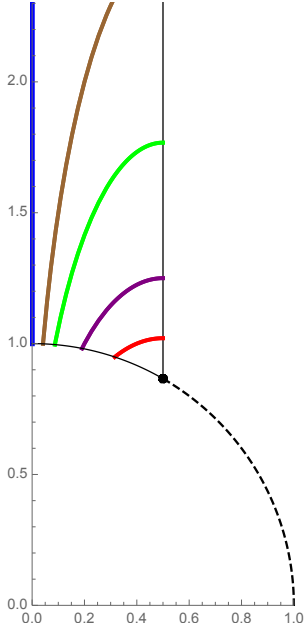


Fig. 6. Level curves of $P_e = k$, in left-right ordering, for $k = 0, k = 0.01, k = 0.02, k = 0.04, k = 0.06$ and $k = 1/12 \approx 0.0833$. Notice that a is represented in the horizontal axis and b in vertical axis.

B. Rate Computation for a Babai Partition

Rate calculations are provided and high rate (small α) approximations are made for both communication models. We may also consider here a lattice generated by a matrix in an upper triangular form (obtained via QR decomposition from a good basis - Minkowski-reduced basis or at least LLL basis).

1) *Centralized Model:* We now describe the transmission protocol Π_c by which the nearest plane lattice point can be determined at the fusion center F . Let $v_{m,l}/v_{m,m} = p_{m,l}/q_{m,l}$ where $p_{m,l}$ and $q_{m,l} > 0$ are relatively prime. Note that we are assuming the generator matrix is such that the aforementioned

ratios are rational, for $l > m$. Let $q_m = \text{l.c.m.} \{q_{m,l}, l > m\}$, where l.c.m. denotes the least common multiple of its argument. By definition $q_n = 1$.

Protocol 1. (Transmission, Π_c). Let $s(m) \in \{0, 1, \dots, q_m - 1\}$ be the largest s for which $[x_m/v_{m,m} - s/q_m] = [x_m/v_{m,m}]$. Then node m sends $\tilde{b}_m = [x_m/v_{m,m}]$ and $s(m)$ to F , $m = 1, 2, \dots, n$ (by definition $s(n) = 0$).

Let $\bar{b} = (b_1, b_2, \dots, b_n)$ be the coefficients of λ_{np} , the Babai point.

Theorem 2. *The coefficients of the Babai point \bar{b} can be determined at the fusion center F after running transmission protocol Π_c .*

Proof: Observe that each coefficient of \bar{b} is given by

$$b_m = \left\lfloor \frac{x_m - \sum_{l=m+1}^n b_l v_{m,l}}{v_{m,m}} \right\rfloor, m = 1, 2, \dots, n, \quad (6)$$

which is written in terms of $\{z\}$ and $\lfloor z \rfloor$, the fractional and integer parts of real number z , resp., ($z = \lfloor z \rfloor + \{z\}$, $0 \leq \{z\} < 1$) by

$$b_m = \left\lfloor \frac{x_m}{v_{m,m}} - \left\{ \frac{\sum_{l=m+1}^n b_l v_{m,l}}{v_{m,m}} \right\} \right\rfloor = \left\lfloor \frac{\sum_{l=m+1}^n b_l v_{m,l}}{v_{m,m}} \right\rfloor, m = 1, 2, \dots, n. \quad (7)$$

Since the fractional part in the above equation is of the form s/q_m , $s \in \{0, 1, \dots, q_m - 1\}$, where q_m is defined above, it follows that $0 \leq s/q_m < 1$. Thus

$$b_m = \begin{cases} \tilde{b}_m - \left\lfloor \frac{\sum_{l=m+1}^n b_l v_{m,l}}{v_{m,m}} \right\rfloor, & s \leq s(m), \\ \tilde{b}_m - \left\lfloor \frac{\sum_{l=m+1}^n b_l v_{m,l}}{v_{m,m}} \right\rfloor - 1, & s > s(m). \end{cases} \quad (8)$$

can be computed in the fusion center F in the order $m = n, n-1, \dots, 1$. ■

Corollary 2. *The rate required to transmit $s(m)$, $m = 1, 2, \dots, n-1$ is no larger than $\sum_{i=1}^{n-1} \log_2(q_i)$ bits.*

Thus the total rate for computing the Babai point at the fusion center F under the centralized model is no larger than $\sum_{i=1}^n h(p_i) - \log_2 |\det V| - n \log_2(\alpha) + \sum_{i=1}^{n-1} \log_2(q_i)$ bits, where $h(p_i)$ is the differential entropy of random variable X_i , and scale factor α is small. Thus the incremental cost due to the $s(m)$'s does not scale with α . However when α is small, this incremental cost can be considerable, if the lattice basis is not properly chosen as the following examples illustrate.

Example 2. *Consider the hexagonal A_2 lattice generated by*

$$V = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{3}}{2} \end{pmatrix}.$$

The basis vectors forms an angle of 60° and applying what we described above we have that the coefficients b_2 and b_1 are given respectively by

$$b_2 = \left\lfloor \frac{x_2}{v_{22}} \right\rfloor = \left\lfloor \frac{2}{\sqrt{3}} x_2 \right\rfloor \quad (9)$$

and

$$b_1 = \left\lfloor \frac{x_1}{v_{11}} - \left\lfloor \frac{b_2 v_{21}}{v_{11}} \right\rfloor \right\rfloor - \left\lfloor \frac{b_2 v_{21}}{v_{11}} \right\rfloor \quad (10)$$

$$= \left\lfloor x_1 - \left\lfloor \left\lfloor \frac{2}{\sqrt{3}} x_2 \right\rfloor \frac{1}{2} \right\rfloor \right\rfloor - \left\lfloor \left\lfloor \frac{2}{\sqrt{3}} x_2 \right\rfloor \frac{1}{2} \right\rfloor. \quad (11)$$

Hence, for any real vector $x = (x_1, x_2)$ we have $\left\lfloor \left\lfloor \frac{2}{\sqrt{3}} x_2 \right\rfloor \frac{1}{2} \right\rfloor = \frac{s}{q}$, with $q = 2$ and $s \in \{0, 1\}$. Node one must then send the largest integer $s(1)$ in the range $\{0, 1\}$ for which $\left\lfloor x_1 - \frac{s(1)}{q_1} \right\rfloor = \lfloor x_1 \rfloor$ and $s(1) = 0$ or $s(1) = 1$ depending on the value that x_1 assumes.

The cost of this procedure, according to Corollary 2, is no larger than $\log_2 q_1 = 1$ bit. Thus the cost of constructing the nearest plane partition for the hexagonal lattice is at most one bit.

Example 3. Suppose a lattice generated by

$$V = \begin{pmatrix} 1 & \frac{311}{1000} \\ 0 & \frac{101}{100} \end{pmatrix}.$$

One can notice that the basis vectors form an angle of approximately 72.89° and they are already Minkowski-reduced. Using the theory developed above we have that

$$b_2 = \begin{bmatrix} x_2 \\ v_{22} \end{bmatrix} = \begin{bmatrix} 100 \\ 101 \end{bmatrix} x_2 \quad (12)$$

and

$$b_1 = \begin{bmatrix} x_1 \\ v_{11} \end{bmatrix} - \left\lfloor \frac{b_2 v_{21}}{v_{11}} \right\rfloor \begin{bmatrix} 1 \\ v_{11} \end{bmatrix} - \left\lfloor \frac{b_2 v_{21}}{v_{11}} \right\rfloor \quad (13)$$

$$= \begin{bmatrix} x_1 - \left\lfloor \left\lfloor \frac{100}{101} x_2 \right\rfloor \frac{311}{1000} \right\rfloor \\ \left\lfloor \frac{100}{101} x_2 \right\rfloor \frac{311}{1000} \end{bmatrix} - \left\lfloor \left\lfloor \frac{100}{101} x_2 \right\rfloor \frac{311}{1000} \right\rfloor \begin{bmatrix} 1 \\ \frac{311}{1000} \end{bmatrix}. \quad (14)$$

Consider, for example, $x = (1, 1)$ then we have that $\left\lfloor \left\lfloor \frac{100}{101} x_2 \right\rfloor \frac{311}{1000} \right\rfloor = \frac{311}{1000} = \frac{s}{q}$. In this purpose, node one sends the largest integer $s(1)$ in the range $\{0, 1, \dots, 999\}$ for which $\left\lfloor x_1 - \frac{s(1)}{q_1} \right\rfloor = \lfloor x_1 \rfloor$ and we get $s(1) = 500$.

This procedure will cost no larger than $\log_2 q_1 = \log_2 1000 \approx 9.96$ and in the worst case, we need to send almost 10 bits to achieve Babai partition in the centralized model.

The analysis here points to the importance of the number-theoretic structure of the generator matrix V in determining the communication requirements for computing x_{np} .

2) *Interactive Model:* For $i = n, n-1, \dots, 1$, node S_i sends $U_i = \left\lfloor (X_i - \sum_{j=i+1}^n \alpha v_{ij} U_j) / \alpha v_{ii} \right\rfloor$ to all other nodes. The total number of bits communicated is given by $R = (n-1) \sum_{i=1}^n H(U_i | U_{i+1}, U_{i+2}, \dots, U_n)$. For α suitably small, and under the assumption of independent X_i , this rate can be approximated by $R = (n-1) \sum_{i=1}^n h(p_i) - \log_2(\alpha v_{ii})$. Normalizing so that V has unit determinant we get $R = (n-1) \sum_{i=1}^n h(p_i) - n(n-1) \log_2(\alpha)$.

IV. CONCLUSION AND FUTURE WORK

We have investigated the closest lattice point problem in a distributed network, under two communication models, centralized and interactive. By exploring the nearest plane (Babai) partition for a given Minkowski-reduced basis, we have determined the probability of error in analytic form in two dimensions. In two dimensions, the error depends on the ratio of the norms of these vectors and on the angle between them. We have also calculated the number of bits that nodes need to send in both models (centralized and interactive) to achieve the rectangular nearest plane partition. We have also demonstrated the importance of proper basis selection, for minimizing the probability of error. One question we are interested in is whether similar results can be derived for greater dimensions. For example, it may be possible to generalize the results derived here to families A_n and D_n for which reduced form bases are already available.

REFERENCES

- [1] E. Agrell, T. Eriksson, A. Vardy and K. Zeger, *Closest Point Search in Lattices*. IEEE Transactions on Information Theory 48(8), 2201-2214. 2002.
- [2] O. Ayaso, D. Shah and M. A. Dahleh, "Information Theoretic Bounds for Distributed Computation Over Networks of Point-to-Point Channels". IEEE Transactions on Information Theory 56(12), pp. 6020-6039. 2010.
- [3] L. Babai. "On Lovász lattice reduction and the nearest lattice point problem". Combinatorica, 6(1), 1-13. 1986.
- [4] T. Berger, *Rate distortion theory: A mathematical basis for data compression*. Prentice-Hall, Englewood Cliffs, NJ, 1971.
- [5] J. H. Conway and N.J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, USA: Springer, 1999.
- [6] S.D. Galbraith, *Mathematics of Public Key Cryptography*. Cambridge University Press, New York. 2012.
- [7] J. Hoffstein, J. Pipher and J. H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, New York. 2008.
- [8] R. Keralapura, G. Cormode, and J. Ramamirtham. "Communication-efficient distributed monitoring of thresholded counts". Proceedings of the 2006 ACM SIGMOD international conference on Management of data, ACM. 2006.
- [9] E. Kushilevitz and N. Nisan, *Communication Complexity*, Cambridge University Press, 1997.
- [10] A. K. Lenstra, H. W. Lenstra and L. Lovász, "Factoring polynomials with rational coefficients". Mathematische Annalen 261(4), 515 1982.
- [11] N. Ma, and P. Ishwar, "Some results on distributed source coding for interactive function computation", IEEE Transactions on Information Theory, vol. 57, No. 9, pp. 6180-6195, Sept. 2011.
- [12] H. Minkowski, "On the positive quadratic forms and on continued fractions algorithms (Über die positiven quadratischen formen und über kettenbruchähnliche algorithmen)". J. Reine und Angewandte Math., vol. 107, 278297 1891.
- [13] A. Orlitsky and J. R. Roche, "Coding for Computing", IEEE Transactions on Information Theory, vol. 47, no. 3, pp. 903-917, March 2001.
- [14] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications". ACM SIGSAM Bulletin 15(1), 37-44. 1981.
- [15] S. A. Ramprasad and G. Caire and H. C. Papadopoulos, "Cellular and Network MIMO architectures: MU-MIMO spectral efficiency and costs of channel state information". Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers, 1811-1818. 2009.
- [16] C.E. Shannon, "A Mathematical Theory of Communication". Bell System Technical Journal, 27(3), 379-423. 1948.
- [17] V. A. Vaishampayan and M. F. Bollauf, "Communication Cost of Transforming a Nearest Plane Partition to the Voronoi Partition," submitted, IEEE Intl. Symp. Inform. Th., Jan. 2017.
- [18] A. C. Yao, "Some Complexity Questions Related to Distributive Computing(Preliminary Report)". Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing, STOC '79, 209-213. 1979.